JOURNAL OF ALGEBRA 134, 28–35 (1990)

Multiple Factorizations by Cyclic Subsets

SÁNDOR SZABÓ

Department of Civil Engineering and Mathematics,
Technical University of Budapest, Stoczek u.2, H-1111 Budapest, Hungary

Communicated by David Goldschmidt

Received October 30, 1988

In connection with multiple tilings of n-dimensional space by unit cubes sharing no complete $(n-1)$-dimensional face it is proved that a finite abelian group can be multiple factorized by non-subgroup cyclic subsets if and only if it is neither cyclic nor the direct sum of cyclic groups of orders p^a, p, ..., p, respectively. © 1990 Academic Press, Inc.

1. INTRODUCTION

Let G be a finite abelian group written additively and let $A_1, ..., A_n, B$ be subsets of G. If each element b of B is expressible in the form

$$b = a_1 + \cdots + a_n, \qquad a_1 \in A_1, ..., a_n \in A_n$$

precisely k ways and each sum $a_1 + \cdots + a_n$ belongs to B, then we say that B is k-factorized by $A_1, ..., A_n$. Let g be a nonzero element of G and q be an integer less than or equal to the order of g. The set of elements

$$0, g, 2g, ..., (q-1)g$$

will be called a *cyclic set* and will be denoted $[g, q]$. If G is the direct sum of cyclic groups of order $r_1, ..., r_m$, respectively, then the m-tuple of integers $(r_1, ..., r_m)$ will be called the *type* of G. A (k, n)-*factorization* is a k-factorization of a finite abelian group by n cyclic subsets. A (k, n)-factorization is *reducible* if there is a subgroup among the factors and otherwise it is called *irreducible*.

H. Minkowski [3] conjectured and G. Hajós [2] proved that $(1, n)$-factorizations are always reducible. The generalization that (k, n)-factorizations are always reducible was proposed by Ph. Furtwängler [1]. For $n \leqslant 3$ it was verified in [1, 2] independently, but the latter exhibited an irreducible (9, 4)-factorization as well. Later R. M. Robinson [4] gave all

0021-8693/90 $3.00

pairs (k, n) for which there exists an irreducible (k, n)-factorization. His result is: If $n \leqslant 3$, then no such (k, n). If $n = 4$, then k is divisible by the square of an odd prime. If $n = 5$, then $k = 3$ or $k \geqslant 5$. If $n \geqslant 6$, then $k \geqslant 2$. He pointed out that finite cyclic groups have only reducible (k, n)-factorizations. However, the problem of giving all groups which have irreducible (k, n)-factorization remained unsolved. The main result of this paper is the characterization of finite abelian groups which have irreducible (k, n)-factorization:

THEOREM. *Every finite abelian group except cyclic groups and groups of type* $(p^a, p, ..., p)$, *where* p *is a prime and* a *is a positive integer, has an irreducible* (k, n)*-factorization.*

2. The Geometrical Background

A (k, n)-*cube lattice* in n-space is a collection of translates of an n-dimensional cube by elements of a vector lattice such that each point of the n-space which is not on the border of any cube is covered by exactly k cubes. The cube lattice is said to be *columnized* if there are two cubes in columns.

There is an intimate one-to-one correspondence between (k, n)-cube lattices and (k, n)-factorizations. Namely, a cube lattice is columnized if and only if the corresponding factorization is reducible. More about this connection and the history of the problem can be found in [5]. Our main result implies that (k, n)-cube lattices whose corresponding groups are cyclic or of type $(p^a, p, ..., p)$ are always columnized.

3. The Proof

The proof is divided into five steps:

(1) Following [4] we describe a test to check whether a collection of cyclic subsets forms a (k, n)-factorization for some k and n.

(2) To find an irreducible (k, n)-factorization for the group G we may restrict the search to the (k, n)-factorizations in which the cardinalities of the cyclic sets are primes. It is not clear a priori whether these primes divide $|G|$. We will show that they do.

(3) The (k, n)-factorizations of cyclic groups and groups of type $(p^a, p, ..., p)$ are reducible.

(4) Groups of types (p^2, p^2) and (p, p, q), where p and q are different primes, have irreducible (k, n)-factorizations.

(5) The above irreducible factorizations can be extended to all groups except cyclic groups and groups of type $(p^a, p, ..., p)$.

We now present the details.

(1) Let G be a finite abelian group, let M be a character of G, and let $[g, q]$ be a cyclic subset. We say that M *is occupied by* $[g, q]$ if

$$[M(g)]^q = 1 \qquad \text{and} \qquad M(g) \neq 1.$$

A necessary and sufficient condition that

$$[g_1, q_1] + \cdots + [g_n, q_n]$$

should be a (k, n)-factorization of G for some k is that each nonprincipal character of G is occupied in at least one of the cyclic sets. (The proof can be found in [4, p. 250].) Note that $[g, q]$ is a subgroup of G if and only if $qg = 0$. Thus if $q_i g_i \neq 0$ for each i, $1 \leqslant i \leqslant n$, then there is no subgroup among the cyclic sets; that is, the factorization is irreducible.

(2) If q is composite, say $q = uv$, where $u, v \geqslant 2$, then

$$[g, q] = [g, uv] = [g, u] + [ug, v]$$

is a 1-factorization. If $[g, q]$ is not a subgroup, that is, if $qg \neq 0$, then the cyclic set $[ug, v]$ cannot be a subgroup since this happens if $vug = 0$. The cyclic subset $[g, u]$ is not a subgroup since $|g| > u$. Taking account of these observations we may suppose that all cyclic sets in an irreducible factorization have prime cardinalities. Now suppose that

$$[g_1, p_1] + \cdots + [g_n, p_n]$$

is a k-factorization of G and that one of the primes $p_1, ..., p_n$, say p_1, does not divide $|G|$. Note that there is no character M of G for which

$$[M(g_1)]^{p_1} = 1 \qquad \text{and} \qquad M(g_1) \neq 1.$$

From the equation, it follows that the order of $M(g_1)$ divides p_1. From the equation and the inequation, it follows that the order of $M(g_1)$ is p_1, so that p_1 would divide the order of G. This means that there is no character of G occupied by $[g_1, p_1]$ and so $[g_1, p_1]$ may be cancelled from the factorization. Of course, after this cancellation (k, n) becomes $(k/p_1, n-1)$.

(3) To prove that a finite cyclic group has only reducible (k, n)-factorizations, let G be a finite cyclic group and let

$$[g_1, p_1] + \cdots + [g_n, p_n]$$

be a k-factorization of G. Since G is cyclic there is a character M of G which defines an isomorphism between G and a cyclic subgroup of the multiplicative group of complex numbers. There must be an i, $1 \leqslant i \leqslant n$, with

$$[M(g_i)]^{p_i} = 1 \qquad \text{and} \qquad M(g_i) \neq 1.$$

But from the first equation it follows that $p_i g_i = 0$, that is, the ith cyclic set is a subgroup.

To prove that groups of type $(p^a, p, ..., p)$, where p is a prime, have only reducible (k, n)-factorizations, suppose that G is a group of type $(p^a, p, ..., p)$ and

$$[g_1, p] + \cdots + [g_n, p]$$

is a k-factorization of G.

Now G is the direct sum of subgroups H and L of types (p^a) and $(p, ..., p)$, respectively. Consider the character M of G which defines an isomorphism between H and a cyclic subgroup of the multiplicative group of complex numbers and which is the principal character over L. Suppose that M is occupied by $[g_i, p]$, that is,

$$[M(g_i)]^p = 1 \qquad \text{and} \qquad M(g_i) \neq 1.$$

Clearly, $g_i = h + l$, $h \in H$, $l \in L$. Now, $1 = [M(g_i)]^p = [M(h)]^p [M(l)]^p = [M(h)]^p$, and so $ph = 0$. This means that $p(h + l) = pg_i = 0$. Thus $[g_i, p]$ is a subgroup.

(4) Let G be a group of type (p^2, p^2), where p is a prime. To construct an irreducible (k, n)-factorization of G we will show that there is a collection of non-subgroup cyclic subsets of G which occupies all nonprincipal characters of G. Let x and y be the basis of G and let ρ be a primitive p^2th root of unity. The reader can readily verify that the character M of G defined by

$$M(x) = \rho^a \qquad \text{and} \qquad M(y) = \rho^b,$$

where $0 \leqslant a \leqslant p^2 - 1$, $0 \leqslant b \leqslant p^2 - 1$, is occupied by the cyclic set $[cx + dy, p]$ if

$$p \mid ca + db \qquad \text{and} \qquad p^2 \nmid ca + db. \tag{i}$$

Further, this cyclic subset is not a subgroup if

$$p \nmid c \qquad \text{or} \qquad p \nmid d. \tag{ii}$$

The character M is not the principal character if $(a, b) \neq (0, 0)$. Now, for each $(a, b) \neq (0, 0)$ we give a pair (c, d) which satisfies (i) and (ii). One of the components of (a, b), say a, is nonzero. If $p \mid a$ and $a \neq 0$, then let $c = 1$ and $d = 0$. If $p \nmid a$ and $b = 0$, then let $c = p$ and $d = 1$. Similar choices can be made with a and b interchanged. In the remaining cases both a and b are prime to p. Now let $b = pt + s$, where $1 \leqslant s \leqslant p-1$ and $0 \leqslant t \leqslant p-1$. If $t \leqslant p-2$, then let $c = p - s$ and $d = a$, which means that (ii) is satisfied. But (i) is also satisfied since

$$ca + db = a(p-s) + ba = a(p-s+b) = a(p-s+pt+s) = ap(t+1)$$

and so $ca + db$ is a multiple of p but not of p^2 because $a(t+1)$ is prime to p. If $t = p-1$, then let $c = 2p - s$ and $d = a$. Therefore,

$$\begin{aligned} ca + db &= a(2p-s) + ba = a(2p-s+b) \\ &= a(2p-s+p(p-1)+s) = ap(p+1). \end{aligned}$$

We turn to the case of the groups of type (p, p, q), where p and q are different primes. Let G be a group of type (p, p, q) with a basis x, y, and z of orders p, p, and q, respectively. Let ρ and σ be primitive pth and qth roots of unity, respectively. Consider the nonprincipal character M of G defined by

$$M(x) = \rho^a, \qquad M(y) = \rho^b, \qquad M(z) = \sigma^c,$$

where $0 \leqslant a, b \leqslant p-1$ and $0 \leqslant c \leqslant q-1$. Let $g = dx + ey + fz$, where $0 \leqslant d, e \leqslant p-1$ and $0 \leqslant f \leqslant q-1$.

The character M is occupied by the non-subgroup cyclic subset $[g, p]^-$ if

$$[M(g)]^p = 1, \qquad M(g) \neq 1, \qquad pg \neq 0,$$

that is, the following three conditions are fulfilled:

$$p \mid p(da + eb) \quad \text{and} \quad q \mid pfc \tag{i}$$

$$p \nmid da + eb \quad \text{or} \quad q \nmid fc \tag{ii}$$

$$p \nmid pd \quad \text{or} \quad p \nmid pe \quad \text{or} \quad q \nmid pf. \tag{iii}$$

After inspecting these conditions we have the constraints

$$q \mid fc \tag{i}$$

$$p \nmid da + eb \tag{ii}$$

$$q \nmid f. \tag{iii}$$

Combining (i) and (iii), we conclude that

$$c = 0 \tag{i}$$

$$p \nmid da + eb \tag{ii}$$

$$q \nmid f. \tag{iii}$$

Thus if $(a, b) \neq (0, 0)$, $c = 0$, and $f = 1$, then the character M is occupied by a suitable non-subgroup cyclic subset $[g, p]$. Indeed, for $b \neq 0$, let $d = 0$ and $e = 1$; for $a \neq 0$, let $d = 1$ and $e = 0$.

The character M is occupied by the non-subgroup cyclic set $[g, q]$ if

$$[M(g)]^q = 1, \qquad M(g) \neq 1, \qquad qg \neq 0,$$

which are equivalent to the conditions

$$p \mid q(da + eb) \quad \text{and} \quad q \mid qfc \tag{i}$$

$$p \nmid da + eb \quad \text{or} \quad q \nmid fc \tag{ii}$$

$$p \nmid qd \quad \text{or} \quad p \nmid qe \quad \text{or} \quad q \nmid qf. \tag{iii}$$

After simplification these constraints become

$$p \mid da + eb \tag{i}$$

$$q \nmid fc \tag{ii}$$

$$p \nmid d \quad \text{or} \quad p \nmid e. \tag{iii}$$

The character M has already been covered if $c = 0$ so we suppose that $c \neq 0$. Let $f = 1$, which together with $c \neq 0$ satisfies (ii). For each (a, b), $0 \leqslant a$, $b \leqslant p - 1$, we need a $(d, e) \neq (0, 0)$, $0 \leqslant d$, $e \leqslant p - 1$, such that $p \mid da + eb$. If $a = 0$, then let $d = 1$ and $e = 0$. Similarly, if $b = 0$, then let $d = 0$ and $e = 1$. When both a and b are prime to p, then let $d = 1$ and let e be the solution of the congruence $eb \equiv -a$ (modulo p), which has a solution since b is prime to p.

(5) In this step we will show that the above irreducible (k, n)-factorizations can be extended to all finite abelian groups except cyclic groups and groups of type $(p^a, p, ..., p)$. Let G be a finite abelian group. By the fundamental theorem of finite abelian groups, G is the direct sum of cyclic groups of prime power orders, $G = G_1 + \cdots + G_r$, where G_i is cyclic and

$$|G_i| = p_i^{n_i}, \qquad 1 \leqslant i \leqslant r.$$

(The pimes p_i are not necessarily different.) Consider subgroups

$$H_1 \subset G_1, \ldots, H_s \subset G_s,$$

where $s \leqslant r$. The subgroups are assumed to be nontrivial (that is, to have more than one element). We prove that if the subgroup $H = H_1 + \cdots + H_s$ has an irreducible (k, n)-factorization then so does G for some new values of k and n. To prove this, let $g_1, \ldots, g_r$ be generators of $G_1, \ldots, G_r$, respectively. Note that

$$G_1 = [g_1, p_1] + [p_1 g_1, p_1^{t_1 - 1}]$$

is a 1-factorization of G_1 and the second cyclic subset is a cyclic group of order $p_1^{t_1 - 1}$. So it can be factorized in a similar way until the remaining subgroup is equal to H_1. Thus we get the factorization

$$G_1 = [g_1, p_1] + [p_1 g_1, p_1] + \cdots + [p_1^{u_1} g_1, p_1] + G_1',$$

where $G_1' = H_1$ and, similarly,

$$G_i = [g_i, p_i] + [p_i g_i, p_i] + \cdots + [p_i^{u_i} g_i, p_i] + G_i',$$

where $G_i' = H_i$ for $1 \leqslant i \leqslant s$. For $s + 1 \leqslant i \leqslant r$ we consider the same type of factorizations but for them G_i' is chosen to be a cyclic group of order p_i. Thus G has a 1-factorization in the form $G = A + H + B$, where A is 1-factorized by non-subgroup cyclic subsets,

$$H = G_1' + \cdots + G_s' \qquad \text{and} \qquad B = G_{s+1}' + \cdots + G_r'.$$

If $s + 1 \leqslant j \leqslant r$, then we have

$$H + G_j' = H + [g_j', p_j] = H + [g_j' + h, p_j]$$

for any h in H. If we choose h so that $p_j h \neq 0$, then an irreducible (k, n)-factorization of H leads to an irreducible $(k, n + 1)$-factorization of $H + G_j'$ with the same k. Since groups of type $(p_j, \ldots, p_j)$ have only reducible (k, n)-factorization, H is not of this type and so there is an h in H with $p_j h \neq 0$. In this way each G_j' can be replaced by a non-subgroup cyclic set. Using (3), (4), and (5) we now can complete the proof of the main result. Let G be a group of type

$$(p_1^{a(1,1)}, \ldots, p_1^{a(1,s_1)}, \ldots, p_u^{a(u,1)}, \ldots, p_u^{a(u,s_u)}),$$

where $p_1, \ldots, p_u$ are different primes and

$$a(i, 1) \geqslant \cdots \geqslant a(i, s_i) \geqslant 1$$

for $1 \leqslant i \leqslant u$. First suppose that $u = 1$. If $s_1 = 1$ or $s_1 \geqslant 2$ but $a(1, 2) = \cdots = a(1, s_1) = 1$, then by (3), G has only reducible (k, n)-factorizations. Otherwise $a(1, 2) \geqslant 2$ and according to (4) and (5) its subgroup H of type (p_1^2, p_1^2) provides an irreducible (k, n)-factorization for G. Now suppose that $u \geqslant 2$. If $s_1 = \cdots = s_u = 1$, then G is cyclic and has only reducible (k, n)-factorizations. Otherwise $s_i \neq 1$ for some $1 \leqslant i \leqslant u$, say $s_1 \geqslant 2$, then G has a subgroup H of type (p_1, p_1, p_2) and therefore G has an irreducible (k, n)-factorization. This completes the proof.

REFERENCES

1. PH. FURTWÄNGLER, Über Gitter konstanter Dichte, *Monatsh. Math. Phys.* **43** (1936), 281–288.
2. G. HAJÓS, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, *Math. Z.* **47** (1942), 427–467.
3. H. MINKOWSKI, "Geometrie der Zahlen," Leipzig, 1896.
4. R. M. ROBINSON, Multiple tilings of n-dimensional space by unit cubes, *Math. Z.* **166** (1979), 225–264.
5. S. K. STEIN, Algebraic tiling, *Amer. Math. Monthly* **81** (1974), 445–462.